Protecting America with Information Technology

Effective use of information technology can improve the management and functions of the Department of Homeland Security (DHS) and strengthen counterterrorism programs and initiatives. Effectively managed, information technology can transform how we protect the homeland. Unfortunately, the Administration is not sufficiently taking advantage of information technology for homeland security needs, DHS information technology management is not nearly as effective as it needs to be, and DHS has not done enough to make our innovative private sector a full partner in defending the homeland.

One of the principal reasons for creating the Department of Homeland Security (DHS) was to fully integrate and coordinate disparate agencies that share the mission of protecting the homeland. The creation of DHS brought together 22 agencies and more than 180,000 employees into an organization that inherited as many as 8,000 information technology applications.[1] One hundred of these are considered major,[2] such as systems for threat identification and management, incident response, law enforcement, warning and alert communications, port of entry/exit management, and immigration. Effectively using information technology and building communications infrastructure is critical to fulfilling DHS's mission.[3] According to The Brookings Institution, "information technology should represent perhaps the highest priority for homeland security efforts."[4]

Information technology can improve and strengthen counterterrorism programs and initiatives. For example, it can help speed the integration of terrorist watch lists, strengthen the security of our borders by improving our ability to spot fraudulent documents, and greatly improve information sharing and our ability to "connect the dots" among federal, state, and local governments, law enforcement, the intelligence community, and the private sector.

Using information technology effectively is also essential for DHS to operate as a unified organization. Smart investments in information technology to rationalize disparate or duplicative financial and personnel systems will boost DHS's effectiveness by giving its executives greater knowledge and control of DHS resources. For rank-and-file employees, delays or deficiencies in implementing common systems such as e-mail, directory services, payroll and benefits reduce worker productivity.

[1] DHS Chief Information Officer, Steven Cooper, speaking to the Commonwealth of Virginia IT Symposium 2003, as reported in Susan Menke, "At Virginia IT Summit, Cooper Says DHS Has Far to Go," *Government Computer News,* September 29, 2003.

[2] DHS Chief Information Officer, Steven Cooper, testimony before the House Government Reform Committee, "Hearing on Assessing Barriers to Information Sharing in the Department of Homeland Security," May 8, 2003.

[3] Information technology integration is identified by the DHS Inspector General's Office as among the top management challenges facing DHS. See DHS Office of the Inspector General, *Major Management Challenges Facing the Department of Homeland Security,* (Washington, DC: DHS, March 18, 2003). See also, Information Technology Association of America (ITAA), Enterprise Solutions Division, "IT Top Ten War on Terrorism Issues," (Arlington, VA: ITAA, Winter 2003).

[4] M. O'Hanlon, P. Orszag, I. Daalder, et al, *Protecting the American Homeland: One Year On,* (Washington, DC: The Brookings Institution, 2002, with a new preface, January, 2003), xix.

Finally, the information technology capabilities of our private sector are a unique and powerful competitive strength of the American economy. Technology skill and innovation have transformed America's economic productivity and warfighting capability over the past decade. The government must ensure that the private sector's technology expertise is a full partner in our efforts to protect the nation and fight terrorism.

SECURITY GAP: The Administration is Not Doing Enough to Take Advantage of Information Technology for Homeland Security Needs.

Secretary Ridge has stated that the Administration is using new technologies, a restructured homeland security organization, and streamlined processes to make the nation significantly more secure.[5] To be sure, DHS has begun to make modest progress in some areas. For example, the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program has begun using biometrics to verify visa-holder identity at selected ports of entry. The Department's Chief Information Officer (CIO), Steven Cooper, has produced an initial draft of an Enterprise Architecture to serve as a strategic guidance document for its information-technology integration efforts.

Notwithstanding these steps, however, significant problems remain. According to the bipartisan Congressional Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 (Joint Inquiry), while information technology remains one of this nation's greatest advantages, it has not been "fully [or] effectively applied in support of U.S. counterterrorism efforts."[6] Persistent problems include "a reluctance [by the government and the intelligence community] to develop and implement new technical capabilities aggressively," a "reliance on outdated and insufficient technical systems," and "the absence of a central counterterrorism database."[7]

Specifically, according to DHS CIO Cooper:

> Databases used for law enforcement, immigration, intelligence, public health surveillance, and emergency management have not been integrated in ways that allow us to comprehend each others' data or "connect the dots" to better prevent terrorist attacks and protect our people and infrastructure from terrorism. Technologies and cultures of agencies have [led] to 'islands of technologies' and barriers to information integration.[8]

According to The Brookings Institution, "the Administration still has no plan for quickly improving real-time information sharing… among the [broad] set of public and private actors

[5] DHS Secretary, Tom Ridge, speech at the American Enterprise Institute, as reported in Dan Verton, "Ridge sees technology, agency restructuring bolstering homeland security: The head of Homeland Security says the nation is more secure than in 2001," *Computer World*, September 2, 2003.

[6] House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, "Congressional Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001," (Joint Inquiry), December, 2002.

[7] Ibid.

[8] DHS Chief Information Officer, Steven Cooper, testimony before the House Government Reform Committee, "Hearing on Assessing Barriers to Information Sharing at the Department of Homeland Security," May 8, 2003.

who are vital to preventing to homeland attacks."[9] Similarly, the Markle Foundation Task Force on National Security in the Information Age (Markle Foundation) concluded that, "the government's progress since September 11, 2001, toward building an adequate network has been slow and is not guided by an overall vision."[10] The Council on Foreign Relations Independent Task Force on America's Response to Terrorism echoes these concerns and points out the critical need for the federal government to comprehensively implement information technology-system upgrades and systems integration in support of counterterrorism activities:

> The federal government is ill equipped to perform data sharing and filtering tasks among federal agencies in Washington, much less mount an integrated counter-terror information technology campaign [with] state and local governments…. [It] will take years to specify and then implement, given the scale of these upgrades, the overhang of legacy computer systems, and the straightjacket of federal procurement procedures.[11]

The Administration's ability to create a unified terrorist watch list is the test case of its ability to deploy information technology to improve homeland security. There is strong bipartisan consensus on the urgent need to implement a unified terrorist watch list, and the problem was well recognized even before September 11. Watch list data from federal agencies is finite and reasonably well-defined (12 lists at nine agencies). The amount of data that needs to be integrated is significantly smaller than databases that are integrated on a regular basis in the private sector. The technology to succeed is readily available commercially.[12] Properly managed, technology-related aspects of integrating the watch lists should take no more than six to twelve months.[13]

Two-and-a-half years after September 11, however, the Administration has not succeeded in creating a comprehensive unified terrorist watch list supported by a robust integrated database that connects it in real time to all relevant stakeholders. While responsibility for integrating terrorist watch lists briefly resided at DHS, the task has now been assumed by the Terrorist Screening Center (TSC), which is part of the FBI.[14] The failure to complete this basic and important information-sharing task casts serious doubt on the Administration's ability to manage information technology projects generally.

[9] M. O'Hanlon, P. Orszag, I. Daalder, et al, *Protecting the American Homeland: One Year On*, (Washington, DC: The Brookings Institution, 2002, with a new preface, January, 2003), xiv.

[10] Markle Foundation Task Force on National Security in the Information Age, "Task Force Says Government Has Not Yet Taken Advantage of America's Technology Expertise to Combat Terrorism," press release, Markle Foundation, December 2, 2003.

[11] James J. Shinn and Jan M. Lodal, Council on Foreign Relations (CFR) Independent Task Force on America's Response to Terrorism, *Red-Teaming the Data Gap*, (New York, NY: CFR, April, 2002).

[12] Ibid.

[13] Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force*, "Working Group Analyses, Working Group I: Networking of Federal Government Agencies with State and Local Government and Private Sector Entities" and "Appendix G," (New York: Markle Foundation, December 2, 2003), 144. House Select Committee on Homeland Security interviews with various technology-industry experts and data integration experts.

[14] GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing, GAO-03-322*, (Washington: U.S. General Accounting Office, April 15, 2003). The White House, "New Terrorist Screening Center Established," September 16, 2003. http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html.

Within DHS itself, the Administration is facing problems in a number of critical areas. DHS is falling short on integrating basic systems that would improve the Department's daily operations and ensure that DHS is unified, well-run, and greater than the sum of its parts. In addition, border management systems suffer from data quality and availability problems, obsolescence, duplication, and a failure to exploit modern communications technologies.[15]

Despite its promises to "[merge] the personnel and pay systems of all DHS component agencies into a single system," and that, "the new system will be completed by the end of the [2003],"[16] DHS has still not integrated and streamlined basic "back-office" systems within the Department, including important administrative functions like accounting, acquisition, procurement, grant management, asset management, and budgeting.[17] As a result, the DHS may not even know how many employees it has at any given time. According to DHS CIO Cooper, "The Department keeps a running hand-tallied list of its staff, with the total varying from 190,000 to 225,000 depending on which of the 22 component agencies' 24 human resources systems are consulted."[18] Furthermore, many Homeland Security employees continue to rely on their former agencies for important everyday functions like benefits[19] and payroll. Outsourcing functions to other agencies can cost American taxpayers more, as other agencies charge DHS overhead and management fees for providing such services.[20]

The President's fiscal year 2005 budget includes $102.5 million to support the creation of new human-resources systems and initiatives and also funds five new employees for the Business Transformation Office to assist in consolidating management processes, systems, and services. Nonetheless, DHS predicts that a central administrative system "may be years away," and acknowledges that DHS officials are just beginning to "set the initial requirements for the merger project."[21]

Overall, the inability of DHS to effectively streamline its myriad systems slows and undermines the ability of the Department to "build employee and organizational identity and support" and "define the culture," factors highlighted by the GAO as critical to the Department's overall success.[22]

[15] Data Management Improvement Act (DMIA) Task Force, *DMIA Task Force, Second Annual Report to Congress*, "Appendix: IT Summary Report," (Washington, DC: DHS, December 2003).

[16] U.S. Department of Homeland Security, "DHS Announces New 'U.S. VISIT System' for Travelers as the Department Marks Its First 100 Days," press release, April 29, 2003.

[17] Wilson Dizard, "DHS plan for Consolidating Back-Office Apps Emerges," *Government Computer News*, January 26, 2004.

[18] Susan Menke, "At Virginia IT Summit, Cooper Says DHS has Far to Go," *Government Computer News*, September 29, 2003.

[19] DHS Office of the Inspector General, memo in response to questions from the House Select Committee on Homeland Security, January 7, 2004. For example, ODP is obtaining administrative support from the DOJ-OJP; FPS is obtaining administrative support from the GSA; and the TSA obtains support services from the FAA. Also see, for example, memoranda of understanding between DHS and 1) the Department of Treasury, dated March 11, 2003; 2) the Department of Health and Human Services, dated February 28, 2003; and 3) the Department of Transportation, dated February 27, 2003.

[20] Ibid.

[21] Catherine Santana, Director of the DHS Resource Management Transformation Office, from Wilson Dizard, "DHS plan for Consolidating Back-Office Apps Emerges," *Government Computer News*, January 26, 2004.

[22] GAO, *Major Management Challenges and Program Risks: Department of Homeland Security*," GAO-03-102, (Washington, DC: GAO, January, 2003), 8.

In the area of border protection, a team from the Los Alamos National Laboratory, as part of DHS's Data Management Improvement (DMIA) Task Force, recently analyzed all of the information-technology systems within the federal government involved in border control.[23] Nearly all of these systems now reside within DHS.[24] The DMIA concluded that border management systems suffer from the following problems:

- A wide range of data transfer connections exist that could seriously hamper the availability and timeliness of critical information to relevant systems;

- Most systems are obsolete because they are based on outdated technologies; modern communications technologies have not been fully exploited by any of the border management systems.

- Obsolete systems suffer from overlapping or duplicative operational capabilities; suffer from high maintenance costs; have extremely limited interoperability; and have little, if any, adaptability for emergencies, unexpected situations, or changing national priorities.

SECURITY RECOMMENDATION

When it comes to using information technology to improve homeland security, the Administration should have as its goal nothing less than "network-centric homeland security," akin to "network centric warfare" which proved so successful in the Iraq War.[25] In practical terms, this means transforming DHS through the extensive use of up-to-date information technologies to more broadly and efficiently gather and disseminate information to field and headquarters personnel, allowing them to most effectively fulfill their homeland security mission.

Specifically, the Administration should follow the recommendation of the Markle Foundation to create, "a distributed information technology network to share terrorism-related information among federal, state, and local government agencies and the private sector."[26] The

(Continued on following page)

[23] DMIA Task Force, *DMIA Task Force, Second Annual Report to Congress*, "Appendix: IT Summary Report," (Washington, DC: DHS, December, 2003).

[24] Beyond systems remaining at the Departments of State and Justice, nearly all of these systems are now within DHS, including IT systems from the Immigration and Naturalization Services, U.S. Customs, U.S. Coast Guard, Transportation Security Administration, and about 18 other federal agencies.

[25] For general discussion of the effect of technology on American military and security strategy see Stan Crock, Paul Magnussen, and Lee Walczak, "The Doctrine of Digital War," *Business Week*, April 7, 2003. For a more technical discussion on network-centric warfare, see Office of the Assistant Secretary of Defense, Command and Control Research Program (CCRP), Department of Defense, http://www.dodccrp.org/NCW/ncw_chapter.htm.

[26] Markle Foundation Task Force on National Security in the Information Age, "Task Force Says Government Has not Yet Taken Advantage of America's Technology Expertise to Combat Terrorism: Markle Task Force Addresses Actions Needed to Create Information Network to Enhance Security While Preserving Civil Liberties," press release, the Markle Foundation, December 2, 2003.

Administration should rapidly create, by the deadlines promised,[27] a unified comprehensive terrorist watch list which is supported by a robust database that integrates all relevant information on terrorists from across the federal government. DHS should speed the integration of back-office systems, which will be critical to developing organizational unity and effective management within DHS. With respect to border systems, DHS should follow the recommendations of its own task force, the DMIA, to 1) streamline access to information; 2) determine the security benefits of integrating systems across agencies; 3) ensure the quality of data within database systems; 4) proactively avoid the obsolescence of technology; and 4) ensure that "new" systems are designed to easily accommodate change.[28]

SECURITY GAP: DHS Management of Information Technology is Weak.

While many of the information-technology problems facing DHS are to be expected given the size and complexity of the bureaucratic reorganization, the situation is made worse by 1) the organizational weakness of the Department's Management Directorate; 2) instability and attrition within division-level information-technology management; and 3) the lack of a dedicated and robust information technology integration team.

Part of the Department's less-than-effective information technology effort stems from an organizationally weak DHS CIO's office, which resides within the Management Directorate. The DHS CIO currently has little or no direct authority over the divisional CIOs within the Department and the hundreds of disparate legacy systems and projects that they manage.[29] The problem was described in recent testimony before the House Committee on Small Business. According to Patricia Driscoll, CEO of Frontline Defense Systems:

> Recently, the Bureau of Citizenship and Immigration Services [BCIS] let out a [blank purchase agreement] worth $500 million, [which] included anything [IT related] that BCIS intends to buy over the next few years. The way [it] is currently [written], it will exclude any small business…. [It] was put on the street after the CIO of Homeland Security, Steve Cooper, said that he did not want [it] to go out. Mr. Cooper and Undersecretary for Management, Janet Hale, said [it] did not fit the new departmental guidelines' investment plan for IT or strategy for acquisitions… and would severely hurt the small business initiative put forward by the White House. What is the point of having a CIO if he is not given budget control over the Department's IT? Giving him control of the IT money is the only way that that we are going to see the Department start behaving differently and the only way we are going to see some real initiatives on sharing

[27] Terrorist Screening Center Director, Donna Bucela, staff briefing for the House Select Committee on Homeland Security, January 15, 2004. Deadlines described were for a test-phase database containing 60,000 records by the end of March, 2004 and a "final" database by June, 2004. Secretary Tom Ridge testified before the Senate Committee on Government Affairs on February 9, 2004 that names will be "aggregated into a single database" by the end of summer, 2004.

[28] DMIA Task Force, *DMIA Task Force, Second Annual Report to Congress*, "Appendix: IT Summary Report," (Washington, DC: DHS, December, 2003).

[29] Wilson Dizard, "Homeland Security Forges a Systems Cadre: A Unified IT Operation Could Take Years to Develop," *Government Computer News*, September 1, 2003: "The extent of [the CIO's] control is far from complete…DHs has not completely centralized its procurement operations, and though major purchases are subject to approval by investment review boards, CIOs in component agencies wield significant power over personnel and investment decisions."

resources.[30]

The Department's Chief Procurement Officer (CPO), also within the Management Directorate, suffers from similar weakness. The CPO does not have direct line authority over the procurement operations of any of the legacy procurement organizations inherited by DHS.[31] Lacking a single authority to make decisions and set policy for contracting activities across DHS, it will be difficult for the Department to improve operating efficiency and ensure that there is not duplication or redundancy among projects and spending across different DHS divisions.[32]

Furthermore, when DHS was created, there was no plan to provide procurement capabilities for the Information Analysis and Infrastructure Protection Directorate, the Science and Technology Directorate, or the Office of the Secretary. Instead, responsibility for contracting operations for those divisions now rests with the CPO's office. As of January, 2004, the CPO's office had only three procurement operations officers.[33] By the CPO's own estimates, the CPO's office should likely have an operational staff of 90-100.[34] Of that number, the CIO's office alone could require approximately 60 contracting operations staff.[35]

DHS procurement offices not under the CPO's direct control are also understaffed. For example, it is estimated that Transportation Security Administration's contracting staff is roughly 70 percent understaffed, Customs and Border Patrol is approximately 10-15 percent understaffed, and the Federal Emergency Management Agency is slightly understaffed.[36] While the President's 2005 budget includes an additional $2.5 million for contract support for DHS's Investment Review Board to help with technical review and program analysis, those resources are not sufficient to address serious resource shortfalls facing the CPO. The DHS may "simply [be] outnumbered by the personnel in its component parts"[37]

[30] House Committee on Small Business, Subcommittee on Rural Enterprise, Agriculture and Technology, "Hearing on Challenges that Small Businesses Face Accessing Homeland Security Contracts," October 21, 2003.

[31] DHS Chief Procurement Officer, Greg Rothwell, staff briefing for the House Select Committee on Homeland Security, January 14, 2004. Legacy procurement organizations that do not report to the CPO include Federal Emergency Management Agency, the Coast Guard, the Secret Service, and the Border and Transportation Security directorate and its constituent offices, the Transportation Security Administration, Customs and Border Protection, Federal Law Enforcement Training Center, and Immigration and Customer Enforcement.

[32] GAO, *Major Management Challenges and Risks: Department of Homeland Security*, GAO-03-102, (Washington, DC: GAO, January, 2003), 17: "DHS will be faced with the challenge of integrating the procurement functions of many of its constituent programs and missions. Early attention to strong systems and controls for acquisitions and related business processes will be critical to ensuring success and maintaining integrity and accountability."

[33] DHS Chief Procurement Officer, Greg Rothwell, staff briefing for the House Select Committee on Homeland Security, January 14, 2004.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Wilson Dizard, "Homeland Security Forges a Systems Cadre: A Unified IT Operation Could Take Years to Develop," *Government Computer News*, September 1, 2003: "According to a study by the transactional records Access Clearinghouse of Syracuse University, in March [2003] the immediate office of secretary Tom Ridge had a staff of only 33, out of the department's total complement of more than 160,000 employees…. Undersecretary for Management Janet Hale had a staff of only 113 to oversee DHS business functions, including Cooper's operations." The Administration's fiscal year 2005 budget requests $17 million for additional DHS headquarters staff, yet, even if approved, such additional personnel will not be largely available until after 2004, and still may not be sufficient.

In addition to a weak CIO's office, other layers of the Department's information-technology management are unstable. According to the DHS Office of the Inspector General, turnover among divisional CIOs since the Department opened its doors has been 45 percent.[38] It is critical that DHS have a "strong and stable implementation team" to manage DHS's integration.[39]

Compounding a weak CIO's office, a weak CPO's office, and unsettled division-level information-technology management, DHS efforts also suffer from the lack of a dedicated information-technology integration team. According to the GAO, it is important to "dedicate an implementation team to manage the transformation process"[40] and that such a team "have direct access and be accountable to top leadership."[41] With strong executive backing from the most senior DHS leadership, such a team would be empowered to prioritize, manage, and implement information technology projects anywhere within DHS. A dedicated integration team would have no allegiance to any particular operating directorate. It would, therefore, be able to on focus on results and on projects of high strategic value to the Department as a whole.

Without such an integration team, "organizational fragmentation, technological impediments, or ineffective collaboration [will] blunt the nation's collective efforts to prevent or minimize terrorist acts."[42] Efforts to streamline or merge DHS systems are likely to be hampered by bureaucratic infighting as managers seek to preserve particular programs or systems in which they have invested or with which they have become accustomed.

DHS CIO Cooper acknowledges the problem:

> Something [I] might have done differently at the start… was to keep the dedicated integration team [that had been formed] at the White House Office of Homeland Security… We dissolved it, but maybe keeping it in place longer would have been beneficial.[43]

Instead of a dedicated integration team with clear authority to initiate and implement important projects, large or small, anywhere within the Department, DHS has a three-tiered investment-management board to review technology projects based largely on project cost.[44] This structure may not be optimally organized to address critical integration issues with the speed and attention they deserve because factors other than dollar size may be significantly more important when deciding which projects to pursue and with what level of urgency. Furthermore, only the top level board, which looks at information-technology projects with life-cycle costs above $200 million, includes senior DHS leadership with *de-facto* department-wide authority. The two

[38] DHS Office of the Inspector General, memo in response to questions from the House Select Committee on Homeland Security, January 7, 2004.
[39] GAO, *Major Management Challenges and Risks: Department of Homeland Security*, GAO-03-102, (Washington, DC: GAO, January, 2003), 9.
[40] Ibid, 7.
[41] Ibid, 9.
[42] Ibid, 17.
[43] Susan Menke, "At Virginia IT Summit, Cooper Says DHS Has Far to Go," *Government Computer News,* September 29, 2003.
[44] The investment threshold levels for each of the boards is as follows: the Investment Review Board reviews capital reviews projects with contractor costs greater than $50 million and IT projects with life-cycle costs greater than $200 million; the Management Review Council reviews projects with capital costs between $5-$50 million and IT projects with the life cycle-costs of $20-$200 million; the Enterprise Architecture Board reviews projects with annual costs of $1-$5 million and life-cycle costs of $5-$20 million.

"lower" boards, which review projects smaller than $200 million, are comprised of the CIO, other Management Directorate executives (the CPO and Chief Financial Officer) or their designees, and divisional representatives. In light of the organizational weakness of the CIO and the CPO, as previously discussed, these two other boards lack sufficient Department-wide authority to prioritize and rapidly implement information-technology projects that are important to the integration of DHS as a whole. As long as DHS lacks a properly structured, nimble, and empowered information-technology integration team, progress with information-technology integration will be unacceptably slow.

SECURITY RECOMMENDATION

The DHS should rapidly strengthen its management and procurement of information technology by strengthening the offices of the Department's CIO and CPO. The Administration should create a specific budget line item and robust budget justification detail for all of DHS's information-technology related spending; supporting detail on projects and programs should be organized by strategic mission, regardless of where within DHS the activities reside. To improve management accountability, improve transparency and facilitate oversight, DHS should establish clear performance goals for information technology projects, set forth clear milestones and timelines, and be in a position to provide regular progress updates on initiatives in relation to those milestones and timelines.[45] Finally, the Administration should follow the recommendation of the Council on Foreign Relations and create an information-technology integration "Red Team," which includes leading private sector experts, to advise the Department on how to accelerate information technology projects and quickly plug critical technology integration gaps.

SECURITY GAP: The Administration is Not Taking Sufficient Advantage of Private-Sector Expertise.

While Secretary Ridge has acknowledged the critical importance of making contracting easier for the nation's innovative technology vendors,[46] DHS has not yet done enough to make it easier for private sector technology companies to work with DHS. In testimony before the House Committee on Small Business, witnesses expressed frustration with the lack of a reliable and comprehensive one-stop online resource to identify existing contract opportunities. According to Benjamin Brink, President and CEO of Data Search Systems:

> [One] of the best business practices which make sense is one-stop shopping. [DHS] says that they are working on that, but [I did] a web search [to find out] where I might do business with the DHS…. [T]he DHS website took me [to] eight or nine agencies [and]

[45] For the importance of timelines and milestones to DHS technology projects, see for example, GAO, *Aviation Security: Computer Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385, (Washington, DC: GAO, February 12, 2004). See also, GAO, *Major Management Challenges and Risks: Department of Homeland Security*, GAO-03-102, (Washington, DC: GAO, January, 2003), 7.

[46] DHS Secretary Ridge, "Protecting the Homeland: The President's Proposal for Reorganizing Our Homeland Defense Infrastructure," testimony before the Senate Committee on the Judiciary, June 26, 2002. According to Secretary Ridge, "The new Department should have flexible procurement policies to encourage innovation and rapid development and operation of critical technologies vital to securing the homeland."

> gave few links to regulations. I could not find anything about HSARPA [the Homeland Security Advanced Research Project Agency]…. [The] website of [Representative Steven Buyer had] far better information on small businesses doing business with the DHS than the DHS did.[47]

At the same hearing, Daniel Lane, CEO of the EMCOM Project stated that:

> [H]ow we normally find out about the contracts is [to] hang out at the Capitol Hill Club…. I find out more stuff down there than I do ever attending any meeting…. Unfortunately I find out about [business opportunities with DHS] in a bar…. We are continuing to check the contracting websites on a day-to-day basis.[48]

SECURITY RECOMMENDATION

The Administration should ensure the rapid creation of a robust, comprehensive, up-to-date, and easy-to-use one-stop resource (web, phone, fax, support) for companies wishing to do business with DHS. The system should serve as both a means of communication with the private sector and as a management tool that allows DHS executives to quickly determine the progress and status of important projects.

[47] House Committee on Small Business, Subcommittee on Rural Enterprise, Agriculture and Technology, "Hearing on Challenges that Small Businesses Face Accessing Homeland Security Contracts," October 21, 2003.

[48] Ibid.